

DETAILED ACTION

1. This action is in response to the amendment filed on 02/19/2010.
2. Claims 1-19 are pending for consideration.

Response to Arguments

3. Applicant's arguments with respect to claims 13-17 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 13-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. Regarding claim 13, the limitations "commitment" and "decommitment" are not clearly defined in the specification.
7. Further regarding claim 13, the preamble of this claim recites a method for signing and encrypting a message M. However, there are no steps in the body of the claim that is related to the signing or encrypting of a message M. Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gentry et al. (US 7353395) (hereinafter Gentry) in view of Deng et al. (US 6910129) (hereinafter Deng).

Regarding claim 13, Gentry discloses a method of signing and encrypting a message M comprising: obtaining an identity-based-encryption (IBE) private key of a user (Gentry: column 9 lines 9-11: system also includes a private key generator...generates...private keys); using the IBE private key to compute, with computing equipment, a commitment to a secret value and a corresponding decommitment (Gentry: column 5 lines 5-27: The public key P_a is the commitment. The secret value is a non-interaction shared secret S_{ab} . The private key S_a is the decommitment).

Gentry discloses using a symmetric key that is based on the IBE private key (Gentry: column 6 lines 29-31 and column 7 lines 16-18). Gentry does not disclose using a symmetric key to encrypt, with computing equipment, at least one of the commitment and the decommitment. However, Deng discloses using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the

decommitment (Deng: column 6, lines 55-57: using a symmetric key to encrypt a key K (i.e., private key)). Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to have included in Gentry the feature of Deng as discussed above to achieve confidentiality when sending a private key over a public network. The symmetric key is used in this situation to protect the private key from exposing it to unauthorized users.

Regarding claim 14, Gentry in view of Deng further discloses wherein using the symmetric key to encrypt comprises: concatenating the decommitment and the message (Deng: column 6, lines 55-57: encrypted message containing original message m and a key k using a symmetric key; and column 12 lines 19-46); and using the symmetric key to encrypt the concatenated decommitment and message (Deng: column 6, lines 55-57; and column 12 lines 19-46).

Regarding claim 15, Gentry in view of Deng further discloses wherein using the symmetric key to encrypt comprises: concatenating an IBE public key with the message and the decommitment (Deng: column 12 lines 19-46); and using the symmetric key to encrypt the concatenated IBE public key, decommitment, and message (Deng: column 12 lines 19-46).

Regarding claim 16, Gentry in view of Deng further discloses wherein computing the decommitment comprises performing multiplication on an elliptic or hyperelliptic curve (Gentry: column 7 lines 50-55: an elliptic curve).

Regarding claim 17, Gentry in view of Deng further discloses computing the symmetric key that is based on the IBE private key by performing a bilinear pairing calculation on an elliptic or hyperelliptic curve (Gentry: column 4 lines 28-41).

Allowable Subject Matter

10. Claims 1-12 and 18-19 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431